IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

HAYWARD INDUSTRIES, INC., Plaintiff, v. BLUEWORKS CORPORATION, BLUEWORKS INNOVATION CORPORATION, NINGBO C.E. ELECTRONIC TECH CO., LTD.; NINGBO YISHANG IMPORT AND EXPORT CO., LTD., Defendants.	Civil Action No. 3:20-cv-00710-MOC-SCR

DECLARATION OF QIAN HANG IN SUPPORT OF DEFENDANTS' OPPOSITION TO PLAINTIFF HAYWARD INDUSTRIES, INC.'S MOTION TO COMPEL

I, Qian Hang, hereby declare as follows:

1. I am lawyer practicing with the firm of Beijing Yingke (Hangzhou) Law Firm and have represented Ningbo Sihu Electronic Technology Co., LTD. in China for several years. I submit this declaration in support of Defendants' Opposition to Plaintiff Hayward Industries, Inc.'s Motion to Compel, filed herewith.

2. I have been asked to provide a legal opinion regarding the requests that Ningbo Sihu Electronic Technology Co., Ltd. and Ningbo Yishang Import & Export Co., Ltd. ("Ningbo Defendants") cooperate with the U.S. court in the disclosure of evidence.

3. Based on my review of the requests, I believe that the discovery requests involve the jeopardization of data security, trade secrets, state secret protection and personal information protection, combined with the current materials under current Chinese Law and would subject the Ningbo Defendants to fines and penalties, including criminal penalties, if they were to respond to the requests without first going through the appropriate legal channels and after evaluation and approval by the relevant departments. I will summarize the relevant laws and treaty provisions below.

Relevant laws and treaty provision:

4. ***Data Security Law of the People's Republic of China***, adopted by the Standing Committee of the National People's Congress Order No. 84 of the President, issued on 2021.06.10, implemented on 2021.09.01, hierarchy: law

a. Article 3 Data, as referred to in this law, means any record of information by electronic or other means. Data processing, including the collection, storage, use, processing, transmission, provision and disclosure of data. Data security means ensuring that data is being effectively protected and lawfully utilized, as well as in a continuous state of security, by taking the necessary measures.

b. Article 36 The competent authorities of the People's Republic of China shall, in accordance with the relevant laws and international treaties and agreements concluded or participated in by the People's Republic of China, or in accordance with the principle of equality and reciprocity, deal with requests from foreign judicial or law enforcement agencies for the provision of data. Organizations or individuals within the territory of the People's Republic of China may not provide data stored in the People's Republic of China to foreign judicial or law enforcement agencies without the approval of the competent authorities of the People's Republic of China.

c. Article 48 Violation of Article 35 of this law, refuses to cooperate with data retrieval, the relevant competent department shall order correction, give a warning, and impose a fine of not less than 50,000 yuan and not more than 500,000 yuan or more, and impose a fine of not less than 10,000 yuan and not more than 100,000 yuan on persons in charge and persons directly responsible.

d. Violate of Article 36 of this law by providing data to foreign judicial or law enforcement agencies without the approval of the competent authorities, the

competent authorities concerned shall give a warning, and may also impose a fine of not less than 100,000 yuan and not more than 1,000,000 yuan, and impose a fine of not less than 10,000 yuan and not more than 100,000 yuan on persons in charge and persons directly responsible; if causing serious consequences, the competent authorities shall impose a fine of not less than 1,000,000 yuan and not more than 5,000,000 yuan, and may also order the suspension of the related business, suspend business for rectification, revoke the related business permit or business license, and impose a fine of not less than 50,000 yuan and not more than 500,000 yuan on persons in charge and persons directly responsible.

5. ***Personal Information Protection Act of the People's Republic of China***, adopted by the Standing Committee of the National People's Congress Order No. 91 of the President, issued on 2021.08.20, implemented on 2021.11.01, hierarchy: law

a. Article 4 Personal information is all kinds of information recorded electronically or by other means relating to an identified or identifiable natural person, excluding anonymized information. The handling of personal information includes the collection, storage, use, processing, transmission, provision, disclosure and deletion of personal information, etc.

b. Article 21 The State establishes a data classified protection system, and implements classified protection of data according to the degree of importance of the data in economic and social development, as well as the degree of harm that will be caused to national security, the public interest, or the lawful rights and interests of individuals and organizations once the data are tampered with, destroyed, leaked, or illegally acquired or illegally utilized. The National Coordination Mechanism for Data Security coordinates the efforts of the relevant departments to formulate a catalog of important data and strengthen the protection of important data.

c. Data relating to national security, the lifeblood of the national economy, important livelihoods, and major public interests belong to the national core data and are subject to a stricter management system.

d. All regions and departments shall, in accordance with the data classified protection system, determine a specific catalog of important data in their own regions and departments, as well as in related industries and fields, and focus on the protection of the data included in the catalog.

e. Article 41 The competent authorities of the People's Republic of China shall, in accordance with the relevant laws and international treaties and agreements concluded or participated in by the People's Republic of China, or in accordance with the principle of equality and reciprocity, handle requests from foreign judicial or law enforcement agencies for the provision of personal information stored within the territory of the People's Republic of China. A processor of personal information shall not provide personal information stored in the territory of the People's Republic of China to a foreign judicial or law enforcement agencies without the approval of the competent authorities of the People's Republic of China.

f. Article 66 Handling of personal information in violation of the provisions of this Law, or handling of personal information without fulfilling the obligations for the protection of personal information as stipulated in this Law, shall be ordered to make corrections by the department responsible for the fulfillment of the duties for the protection of personal information, be given a warning, be confiscated the illegal income, and be ordered to suspend or terminate the provision of the services of the application that handles personal information in violation of the law; and, if it refuses to make corrections, it shall also be imposed a fine of not more than 1,000,000 yuan; and the persons in charge and persons directly responsible shall be fined not less than 10,000 yuan and not more than 100,000 yuan.

g. If any of the violations mentioned in the preceding paragraph cause serious results, the department above the provincial level which performs the duty of personal information protection shall order rectification, confiscate the illegal income, and impose a fine of not more than 50,000,000 yuan or not more than 5% of the turnover of the previous year, and may also order the suspension of the relevant business or suspension of business for rectification, notify the relevant competent department to revoke the relevant business permit or business license; and impose fines of not less than 100,000 yuan and not more than 1,000,000 yuan on the persons in charge and persons directly responsible, and may decide to prohibit them from acting as directors, supervisors, senior management personnel and persons in charge of personal information protection of the relevant enterprises within a certain period of time.

6. ***Cybersecurity Law of the People's Republic of China***, adopted by the Standing Committee of the National People's Congress Order No. 53 of the president, issued on November 07, 2016, and implemented on June 01, 2017, hierarchy: law

a. Article 37 Personal information and important data collected and generated by

operators of critical information infrastructures operating in the People's Republic of China shall be stored within the country. If, due to business needs, it is necessary to provide them outside the country, a security assessment shall be carried out in accordance with the methods formulated by the Cyberspace Administration of China in conjunction with the relevant departments of the State Council; if otherwise provided for by laws or administrative regulations, the provisions thereof shall be complied with.

7. ***Law of the People's Republic of China on Guarding State Secrets***, revised for the second time at the eighth meeting of the Standing Committee of the Fourteenth National People's Congress on February 27, 2024, and implemented as of May 1, 2024, hierarchy: law

a. Article 27 Equipment, products, development, production, transportation, use, preservation, maintenance and destruction belong to the state secrets shall comply with the provisions of state secrecy.

b. Article 28 Organs and units shall strengthen the management of carriers of State secrets, and no organization or individual shall engage in the following acts:
(i) Illegal acquisition and possession of State secret carriers;
(ii) Buying, selling, transferring or privately destroying State secret carriers;
(iii) Transmission of State secret carriers through ordinary postal services, courier services and other channels without confidentiality measures;
(iv) Sending or consigning State secret carriers out of the country;
(v) Carrying or transmitting State secret carriers out of the country without authorization from the competent authorities concerned;
(vi) Other violations of the confidentiality of State secret carriers.

8. ***Civil Procedure Law of the People's Republic of China***, adopted by the Standing Committee of the National People's Congress, issued on 2023.09.01, implemented on 2024.01.01, hierarchy: law.

a. Article 294 Requests for and rendering of legal assistance shall be made in accordance with the channels provided for in international treaties concluded or participated in by the People's Republic of China; if there is no treaty, it shall be made through diplomatic channels.

b. Foreign embassies and consulates in the People's Republic of China may serve documents on citizens of that State and investigate and collect evidence, provided that they do not contravene the laws of the People's Republic of China and that they do not take coercive measures.

c. Except as provided for in the preceding paragraph, no foreign organ or individual may serve documents or investigate and collect evidence within the territory of the People's Republic of China without the permission of the competent authorities of the People's Republic of China.

d. Article 295 A foreign court's request for judicial assistance from the people's court and the documents attached thereto shall be accompanied by a Chinese translation or other language text as provided for in an international treaty.

e. A request by the people's court for judicial assistance from a foreign court and the documents attached thereto shall be accompanied by a translation into the language of that country or other language texts as provided for in international treaties.

f. Article 296 The provision of judicial assistance by the people's court shall be carried out in accordance with the procedures prescribed by the laws of the People's Republic of China. Where a foreign court requests that a special method be used, it may also proceed in accordance with the special method it requests, provided that the special method requested does not violate the laws of the People's Republic of China.

9. ***Methods for Data Export Security Assessment***, Order No. 11 adopted by the Cyberspace Administration of China, issued on 2022.07.07, implemented on 2022.09.01, hierarchy: departmental regulation

a. Article 1 In order to regulate data export activities, protect the rights and interests of personal information, safeguard national security and social public interests, and promote the safe and free transfer of data across borders, the present measures shall be formulated according to the Network Security Law of the People's Republic of China, the Data Security Law of the People's Republic of China and the Personal Information Protection Act of the People's Republic of China and other laws and regulations.

b. Article 4 Data processor to provide data outside the country, one of the following circumstances, should declare the data export security assessment to the Cyberspace Administration of China through local provincial Cyberspace Administration:
(i) Data processors provide important data outside the country;
(ii) Critical information infrastructure operators and data processors handling personal information of more than 1,000,000 people provide personal information outside the country;

(iii) A data processor that has provided 100,000 people's personal information or 10,000 people's sensitive personal information to foreign countries in the aggregate since January 1 of the previous year provides personal information to foreign countries;

(iv) Other cases stipulated by the Cyberspace Administration of China that require the declaration of data export security assessment.

c. Article 5 Data processors shall carry out a self-assessment of data export risk before declaring data export security assessment, focusing on the following matters:

(i) The legality, legitimacy and necessity of the purpose, scope and manner of data processing by the outbound and offshore recipients;

(ii) The scale, scope, type and sensitivity of the outbound data, and the risks that the outbound data may pose to national security, public interests and the legitimate rights and interests of individuals or organizations;

(iii) The responsibilities and obligations that the overseas recipient undertakes to assume, as well as whether the management and technical measures and capabilities for fulfilling the responsibilities and obligations can guarantee the security of the outbound data;

(iv) The risk of data being tampered with, destroyed, leaked, lost, transferred, or illegally obtained or utilized during or after export, and whether the channels for safeguarding the rights and interests of personal information are smooth;

(v) Whether the data export-related contracts or other legally binding documents (hereinafter collectively referred to as legal documents) drawn up with overseas recipients have sufficiently agreed on the responsibility and obligations for data security protection;

(vi) Other matters that may affect the security of data export.

10. ***Frequently Asked Questions on International Judicial Assistance in Civil and Commercial Matters***

a. The Ministry of Justice of the People's Republic of China, on March 30, 2023, in accordance with the provisions of the Hague Service Convention and the Hague Evidence Convention, as well as the 38 Sino-foreign bilateral treaties on legal assistance (hereinafter collectively referred to as the "Treaties") currently in force, provided for the conduct of mutual legal assistance in civil and commercial matters through diplomatic channels, which includes the brief answers to service of judicial documents, the taking of evidence and the recognition and enforcement of judgments.

b. Q: How can foreign judicial organs or judicial personnel access evidence materials located in China?

c. A: Requests for investigation and collection of evidence shall be submitted to the Ministry of Justice by foreign judicial organs or individuals qualified to make such requests, in accordance with the channels provided for in the treaty. Where no relevant treaty has been concluded with China, the request shall be submitted to the Ministry of Foreign Affairs. After approval, the request is executed by the People's Court, and the result is replied to the requesting party by the request receiving department.

d. Q: Can a foreign judicial authority or relevant person commission a lawyer or other institution in China to question witnesses or other persons or access materials located in China and use the results in proceedings in a foreign court?

e. A: According to China's Civil Procedure Law, the taking of evidence shall be conducted by the People's Court or, with the approval of the People's Court, by lawyers, and no other institution or individual may take evidence in China.

Legal Analysis of Chinese Law

11. In response to the United States' wide-ranging discovery program, in the data field, countries around the world have enacted data protection laws to play the role of "blocking regulations" to safeguard national sovereignty, such as the European Union's *General Data Protection Regulation* (hereinafter referred to as the GDPR). China's *Personal Information Protection Act and Data Security Law*, which contain restrictive provisions on cross-border data transfers, and the *Methods for Data Export Security Assessment* also play the same role, and are known as "privacy and data protection laws and regulations that play the role of a blocking statute".

Article 41 of China's *Personal Information Protection Act* and article 36 of the *Data Security Law* stipulate that organizations or processors of personal information shall not provide data or personal information stored in China to foreign judicial or law enforcement agencies without the approval of the competent authorities. As mentioned earlier, the *Civil Procedure Law* also stipulates that judicial assistance/investigation and evidence collection should be conducted with the authorization of the competent authorities of the People's Republic of China. As can be seen, Chinese law imposes strict restrictions on access to evidence in China by overseas law enforcement and judicial authorities. In order to safeguard China's national sovereignty and protect state secrets, the *Data Security Law* imposes heavy legal liabilities for the provision of

domestic data to overseas judicial authorities without legal procedures, such as warnings, suspension business for rectification, revocation of business licenses, and fines of up to millions of yuan. Therefore, enterprises in China must not ignore the above provisions and provide data to overseas jurisdictions in accordance with the law, otherwise they will face heavy legal liabilities.

12. On March 30, 2023, the Ministry of Justice of the People's Republic of China published the *Frequently Asked Questions on International Judicial Assistance in Civil and Commercial Matters* on its official website, which stipulates the export of evidence in the scenario of judicial assistance in civil and commercial matters: if a foreign judicial organ or judicial officer wants to retrieve evidence materials located in China, he or she can't directly interrogate (including by technical means such as telephone and video) witnesses located in China, and should in accordance with the means provided for in the treaty, a foreign judicial organ or individual qualified to make a request for evidence shall submit a request to the Ministry of Justice for investigation and evidence collection. Where no relevant treaty has been concluded with China, the request shall be submitted to the Ministry of Foreign Affairs. The request shall be executed by the People's Court after approval, and the result shall be replied to the requesting party by the request receiving department. The above-mentioned *Frequently Asked Questions on International Judicial Assistance in Civil and Commercial Matters* instructed by China's Ministry of Justice still adheres in practice to the principles of judicial sovereignty and data sovereignty, and prohibits individuals and enterprises within the country from providing evidence to foreign judicial authorities directly upon their request. Since China made a reservation to the provision on judicial evidence collection through diplomatic channels (except for Article 15 "requesting assistance in obtaining evidence directly from the judicial organs of a contracting state through diplomatic or consular officials") when it acceded to the *Hague Evidence Convention* in 1997, foreign cross-border requests for obtaining evidence in civil and commercial matters basically need to be filed with the Ministry of Justice to go through the procedure of judicial assistance in civil and commercial matters. The procedure for judicial assistance in civil and commercial matters is basically required to be submitted to the Ministry of Justice.

Therefore, in accordance with the instructions of the Ministry of Justice of China, it has been clarified that foreign judicial organs retrieving evidence in China should submit their requests to the relevant organs in accordance with the channels stipulated in the *Hague Convention on Access to Evidence Abroad in Civil and Commercial Matters* (the "Hague Convention"), which will be carried out by the courts upon approval. From this, we can also deduce that enterprises in China are not allowed to directly provide data stored in their territories to foreign judicial organs upon request, but should complete the transmission of evidence through designated channels.

13. According to the *Methods for Data Export Security Assessment* issued by the Cyberspace Administration of China, it can be seen that the provision of the following information should be declared to the Cyberspace Administration of China for data export security assessment through the local provincial Cyberspace Administration: (1) Data processors providing important data outside the country; (2) Operators of critical information infrastructures and data processors handling personal information of more than 1,000,000 people providing personal information outside the country; (3) Data processors that have cumulatively provided 100,000 people's personal information or 10,000 people's sensitive personal information to foreign countries since January 1 of the previous year provide personal information to foreign countries; (4) Other circumstances stipulated by the Cyberspace Administration of China that require the declaration of data export security assessment. In light of the fact that the documents served on the Ningbo Defendants through the U.S. court set forth the required evidence disclosure materials, which contain many contents involving state secrets, personal information, and other commercial secret data, and belong to the cases stipulated in the above regulations, the Ningbo Defendants must declare the data export security assessment to the Cyberspace Administration of China through local provincial Cyberspace Administration, or else it may violate the Data Security Law, Personal Information Protection Act and other data law related regulations, which may cause the Ningbo Defendants to face administrative penalties or even criminal sanctions.

14. In summary, in this case, many of Plaintiff Hayward Industries, Inc.'s discovery requests pursuant to the Federal Rules of Civil Procedure (Fed.R.Civ.p.69, N.C. Gen. Stat. §§ 1-352,1 and N.C Gen. Stat. §§ 1-352.2), which involve "important state secrets, trade secret data" and "personal information," fall into the category of data and information that requires the approval of the Chinese authorities or judicial organs before it can be provided. Most of the evidence requested to disclose by the Ningbo Defendants is evidence belongs to the "core data", including data related to national security, important livelihood rights and interests, as well as once leaked and illegally used will jeopardize national security, economic operations, which not only infringes on the commercial secrets of Chinese enterprises, but also jeopardizes the security of state secrets, and is not conducive to the protection of personal information. Therefore, we suggest that Hayward must go through legal channels and obtain the relevant data after evaluation and approval by the relevant departments.

15. The data involved in the materials currently required by in the US court to be provided by the Ningbo Defendants may infringe their trade secrets, or endanger the information

security of others, and even infringe China's international secrets.

16. Some of these issues are no longer within the scope of the Ningbo Defendants' control, and it is indeed difficult to disclose evidence. Many issues even involve infringement of the Ningbo Defendants' trade secrets, the security of state secrets and information security of others. In other words, if the Ningbo Defendants directly submits this information to the U.S. court, they may even face the risk of administrative or even criminal penalties. In this case I am of the opinion that there is a real conflict between Chinese law and U.S. law, and non-compliance with Chinese law will seriously damage China's important national interests.

17. I have assisted the Ningbo Defendants in submitting the discovery requests to the appropriate Chinese authorities for review and permission.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on July 31, 2024

/s/ Qian Hang
Qian Hang
Partner
Beijing Yingke (Hangzhou) Law Firm
Email: qianhang@yingkelawyer.com

Mr. Qian Hang
July 31, 2024